UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,241	01/16/2004	Kristy L. Birt	END920030052US1(1397-9U)	7209

68786 7590 08/16/2011

CHRISTOPHER & WEISBERG, P.A.
200 EAST LAS OLAS BOULEVARD
SUITE 2040
FORT LAUDERDALE, FL 33301

EXAMINER	
ALMEIDA, DEVIN E	
ART UNIT	**PAPER NUMBER**
2432	

MAIL DATE	DELIVERY MODE
08/16/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte KRISTY L. BIRT, JAMES P. GODDARD, and
KERRY L. LAUREN

Appeal 2009-013297
Application 10/759,241
Technology Center 2400

Before GREGORY J. GONSALVES, JASON V. MORGAN, and
BRUCE R. WINSOR, *Administrative Patent Judges*.

MORGAN, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Introduction

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 10, 11, 21, 22, 25, and 26.[1] We have jurisdiction under 35 U.S.C. § 6(b).

Exemplary Claim

> 10. A method for determining a criticality factor for a security vulnerability in a computer system, comprising:
>
> entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment;
>
> measuring a frequency of occurrence for the detected security vulnerabilities; and
>
> assigning a security vulnerability factor to a detected security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system.

(Claims App'x B – C)

Rejections and Appellants' Contentions

Appellants contend that the Examiner erred in rejecting claim 10 under 35 U.S.C. § 103(a) as being unpatentable over Keir (US 7,243,148 B2), Bellemore (US 5,944,825), and Dahlstrom (US 2004/0006704 A1) because:[2]

> The preamble of Claim 10 recites "a method for determining a criticality factor for *a security vulnerability* in a

---

[1] The Examiner has withdrawn the rejections of pending claims 1, 5, 6, 8, 9, 12, 16, 17, 19, 20, 23, and 27 – 30 (Ans. 3).

[2] Separate patentability is not specifically argued for claims 21 and 26, which recite similar features to claim 10.

> computer system" (emphasis added). Thus, the method disclosed in Claim 10 relates to a single security vulnerability. . . . The method disclosed in Keir considers the entire content and makeup of a complete network, including the number and types of security vulnerabilities found, whereas the method recited in Claim 10 relates to a single security vulnerability . . . .
>
> Claim 10 recites the actual function of the frequency score . . . , the criticality score . . . , the severity score . . . , and the trust score . . . . None of the cited references teach, disclose or suggest the recited features.

(App. Br. 14 – 15).

ISSUES

1. Did the Examiner err in finding that the combination of Keir, Bellemore, and Dahlstrom teaches or suggests a method for determining a criticality factor for a security vulnerability in a computer system, as recited in claims 10, 21, and 26?

2. Did the Examiner err in finding that the combination of Keir, Bellemore, and Dahlstrom teaches or suggests an assigned security vulnerability factor based on the claimed sub-factors, as recited in claims 10, 21, and 26?

3. Is the claim recitation "whether information on the element is used for aggregation," found in claims 11, 22, and 25, indefinite under 35 U.S.C. § 112, second paragraph?

ANALYSIS

We have reviewed the Examiner's rejections in light of Appellants' arguments (Appeal Brief) that the Examiner has erred.

We disagree with Appellants' conclusions with respect to claims 10, 21, and 26. With respect to these claims, we adopt as our own (1) the

findings and reasons set forth by the Examiner in the action from which this appeal is taken and (2) the reasons set forth by the Examiner in the Examiner's Answer in response to Appellants' Appeal Brief. Except with respect to claims 11, 22, and 25, we concur with the conclusions reached by the Examiner. With respect to claims 11, 22, and 25, we reverse the Examiner and enter new grounds of rejection.

(1) *Whether the Examiner erred in finding that the combination of Keir, Bellemore, and Dahlstrom teaches or suggests a method for determining a criticality factor for a security vulnerability in a computer system, as recited in claims 10, 21, and 26*

Keir discloses a FoundScore $F=100-V-E$ where

$$V=\min (70, (70V_hH_h+42V_mH_m+14V_lH_l)/H_n)),$$

and where V_h, V_m, and V_l are the number of high, medium, and low level vulnerabilities detected while H_h, H_m, and H_l are the number of hosts on which high, medium, and low level vulnerabilities are detected (col. 64, ll. 20 – 48). Keir encompasses situations where only one vulnerability is detected (e.g., V_h=1, V_m=0, and V_l=0). As such, we do not agree with Appellants that Keir fails to teach or suggest a method for determining a criticality factor for a single (e.g., a high level) security vulnerability.

Accordingly, the Examiner has not erred with respect to this issue in the rejection of claims 10, 21, and 26.

(2) *Whether the Examiner erred in finding that the combination of Keir, Bellemore, and Dahlstrom teaches or suggests an assigned security vulnerability factor based on the claimed sub-factors, as recited in claims 10, 21, and 26*

We do not find any errors in the Examiner's detailed mapping of the teachings and suggestions of Keir to the claimed sub-factors of claims 10, 21, and 26 (Ans. 7 – 8). Moreover, we do not agree with Appellants that

Keir fails to teach determining a security vulnerability based on the isolation of a system. Keir's FoundScore *F* is based on exposure loss *E*, which is based on W_y, the number of wireless access points found on host y (col. 64, ll. 20 – 26; col. 65, ll. 5 – 17). An artisan of ordinary skill would realize that a host having zero wireless access points would be more isolated than a host having many wireless access points. Thus, Keir teaches or suggests isolation of a system (e.g., number of wireless access points found) as a sub-factor in an assigned security vulnerability factor (FoundScore F).

Furthermore, Appellants' arguments based on the "product of" recitation of claim 1 (App. Br. 8 – 10) are not applicable with respect to the rejections of claims 10, 21, and 26. These claims use the broader "based upon" recitation, which is clearly not limited to the mathematical definition of a product.

Accordingly, the Examiner has not erred with respect to this issue in the rejection of claims 10, 21, and 26.

NEW GROUNDS OF REJECTION

(3) *Is the claim recitation "whether information on the element is used for aggregation," found in claims 11, 22, and 25, indefinite under 35 U.S.C. § 112, second paragraph*

The test for definiteness under 35 U.S.C. § 112, second paragraph, is whether "those skilled in the art would understand what is claimed when the claim is read in light of the specification." *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1576 (Fed. Cir. 1986) (citations omitted). In particular, a claim is indefinite if it possesses a claim recitation that is amenable to two plausible definitions and therefore ambiguous. *Ex parte Miyazaki*, 89 USPQ2d 1207, 1215 (BPAI 2008) (precedential).

Claims 11, 22, and 25 recite either a "the criticality of an element in the system" or a "criticality score" that is "based on . . . whether information on the element is used for aggregation" (Claims App'x C, E, and G). The Application provides little guidance as to the meaning of "whether information on the element is used for aggregation," merely indicating that a criticality score of 2 can be used if no confidential or personal data is on a system, but the information on the asset may be used for aggregation (Spec. 16, ll. 16 – 20). We cannot find evidence in the Application clearly describing what the information is and how it may be used for aggregation.

At least two plausible claim constructions of "whether information on the element is used for aggregation" arise from the Application's sparse description: (1) information on the element is used for aggregation if that information describes how to perform the aggregation and (2) information is used for aggregation if that information itself is aggregated (i.e., is a component of an aggregation). The difference between these two interpretations is like the difference between a recipe, which describes how to combine (i.e., aggregate) ingredients to form a dish, and the ingredients themselves, which are components of the dish. Unlike a recipe or ingredients, which each play a distinct role in forming a dish, "information" can mean either something that instructs or something that can be aggregated. It follows that, in the same way that both a recipe and the ingredients can be said to be "used" for making a dish, both of the identified claim constructions of "whether information on the element is used for aggregation" are plausible.

Due to the fact that "whether information on the element is used for aggregation" is amenable to at least two plausible claim constructions, we

enter a new ground of rejection of claims 11, 22, and 25 under 35 U.S.C. § 112, second paragraph. Because these claims are indefinite, the prior art rejections of these claims fall; these rejections necessarily are based on speculative assumptions as to the meaning of the claims. *See In re Steele*, 305 F.2d 859, 862 – 63 (CCPA 1962). It should be understood, however, that our decision in this regard is based solely on the indefiniteness of the claimed subject matter and does not reflect on the adequacy of the prior art evidence applied in support of the rejections.

CONCLUSIONS OF LAW

Based on the findings of facts and analysis above, we conclude that claims 10, 21, and 26 are unpatentable because the Examiner did not err in finding:

1. that the combination of Keir, Bellemore, and Dahlstrom teaches or suggests a method for determining a criticality factor for a security vulnerability in a computer system, as recited in claims 10, 21, and 26, and

2. that the combination of Keir, Bellemore, and Dahlstrom teaches or suggests an assigned security vulnerability factor based on the claimed sub-factors, as recited in claims 10, 21, and 26.

We also conclude that claims 11, 22, and 25 are unpatentable because the claim recitation "whether information on the element is used for aggregation," found in claims 11, 22, and 25, is not definite under 35 U.S.C. § 112, second paragraph.

DECISION

We affirm the Examiner's decisions rejecting claims 10, 21, and 26 under 35 U.S.C. § 103(a).

We reverse *pro forma* the Examiner's decisions rejecting claims 11, 22, and 25 under 35 U.S.C. § 103(a).

We enter a new ground of rejection of claims 11, 22, and 25 under 35 U.S.C. § 112, second paragraph.

37 C.F.R. § 41.50(b) provides that, "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 C.F.R. § 41.50(b) also provides that the Appellants, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new grounds of rejection to avoid termination of proceedings (37 C.F.R. § 1.197 (b)) as to the rejected claims:

(1) Reopen prosecution. Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the proceeding will be remanded to the examiner. . . .

(2) Request rehearing. Request that the proceeding be reheard under 37 C.F.R. § 41.52 by the Board upon the same record. . . .

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

tj